State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

September 8, 2015

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2015-106

DATE(S) ISSUED:
09/08/2015

SUBJECT:
Vulnerability in Windows Media Center Could Allow Remote Code Execution (MS15-100)

OVERVIEW:
A vulnerability has been discovered in Microsoft WindowsMedia Center, which could allow an attacker to take complete control of an affected system. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
This vulnerability has been publicly disclosed, but has not been publicly used to attack users.

SYSTEMS AFFECTED:
- **Microsoft Windows Vista**
- **Microsoft Windows 7**
- **Microsoft Windows 8and 8.1**

RISK:
Government:
- **Large and medium government entities: High**
- **Small government entities: High**

Businesses:
- **Large and medium business entities: High**
- **Small business entities: High**

Home users: High

TECHNICAL SUMMARY:

A vulnerability exists in Windows Media Center that could allow remote code execution if Windows Media Player opens a specially crafted Media Center link (.mcl) file that references malicious code. To exploit this vulnerability, an attacker must entice a user to install the .mcl filed on the local machine. An attacker who successfully exploits this vulnerability could gain the same user rights as the current user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- **Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.**
- **Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.**
- **Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.**
- **Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.**

REFERENCES:
Microsoft:
https://technet.microsoft.com/en-us/library/security/MS15-100

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2509